Electronic Banking

Examiners should evaluate the above-captioned function against the following control and performance standards. The Standards represent control and performance objectives that should be implemented to help ensure the bank operates in a safe and sound manner, and that the entity's objectives are carried out. Associated Risks represent potential threats to the bank if the standards are not achieved and maintained. The Standards are intended to assist examiners in analyzing important functions that may warrant additional review. All of the following Standards may NOT need to be considered at every bank. Conversely, these do NOT represent all of the control and performance standards needed for every bank. Examiners should continue to use their judgement when assessing risk.

Standards	Associated Risks
PERFORMANCE	
Management develops adequate contingency and disaster plans. The bank's internal systems and confidential customer data are adequately protected against attack from both internal and external sources.	The bank could be liable to customers for losses due to system interruptions or malfunctions. Unauthorized parties could obtain access to or compromise confidential bank or customer information. Intrusion attempts may not be detected, contained, and reported in a timely manner, leading to potential loss of critical data.
Adequate due diligence was completed prior to system implementation.	Adequate internal controls may not exist, exposing the bank to uncontrolled security or fraud risks.
Contracts for outsourced electronic banking capabilities are comprehensive, have been thoroughly reviewed by legal staff, and are reviewed and managed on an ongoing basis.	Unanticipated exposure to credit, market, liquidity, legal, operational and reputational risks could result.
MANAGEMENT AND CONTROL	
The board and bank management review policies and procedures, and make appropriate revisions to incorporate electronic banking products and services.	Policies and procedures may not adequately address the impact on bank activities, operations, or security. Existing controls may not adequately protect confidential electronic information.
The board establishes appropriate standards and procedures for overall electronic banking administration and systems operation.	The bank may experience financial losses if the system becomes obsolete or needs to be upgraded more frequently than anticipated. Erroneous information could be provided to customers, exposing banks to legal and reputational risks.
Internal and external audit programs incorporate electronic banking systems.	Potential security, operational, compliance or control weaknesses in electronic banking systems may not be identified.
Information and communication systems ensure that relevant information is identified, processed and reported.	Reporting may be unreliable, compliance with laws, regulations, and internal policies may be jeopardized.
Appropriate management oversight is established to administer outsourcing arrangements.	Electronic banking services could be disrupted if vendors or third-party providers experience financial difficulties.

Standards	Associated Risks
	Vendor may not meet terms of contract, causing financial losses or leading customers to withdraw deposits or close accounts.
Management provides adequate training to employees on proper controls and potential risks associated with alternative delivery and payment systems.	Staff may not implement adequate controls over data integrity, information security, and business resumption plans.
The board or an appropriate committee approves the electronic banking services based on a written business plan that includes a cost/benefit, risk, and financial impact analysis that is commensurate with the activity.	Inadequate planning may result in new electronic banking products or services having unexpected impacts on liquidity, sensitivity to market risk, or loan quality. Investments in electronic banking systems may have unexpected impacts on the bank's earnings or capital.

Electronic Banking

Core Analysis Decision Factors

Examiners should evaluate Core Analysis in this section for significance and to determine if an Expanded Analysis is necessary. Negative responses to Core Analysis Decision Factors may not require proceeding to the Expanded Analysis. Conversely, positive responses to Core Analysis Decision factors do not preclude examiners from proceeding to the Expanded Analysis if deemed appropriate.

Do Core Analysis and Decision Factors indicate that risks are adequately identified, measured, monitored, and controlled?

Core Answer: General Comment:(If any)

Core Analysis Decision Factors

C.1. Are policies and procedures adequate?

C.2. Are internal controls and security adequate?

C.3. Are the audit or independent review functions adequate?

C.4. Are information and communication systems adequate and accurate?

C.5. Is an effective vendor/service provider oversight program in effect?

C.6. Do the board and senior management effectively supervise electronic banking activities?

Electronic Banking

Expanded Analysis Decision Factors

This section evaluates the significance and materiality of deficiencies or other specific concerns identified in the Core and Expanded Analyses.

Do Expanded Analysis and Decision Factors indicate that risks are adequately identified, measured, monitored, and controlled?

Expanded Answer: General Comment:(If any)

Expanded Analysis Decision Factors

E.1. Are management deficiencies immaterial to electronic banking?

E.2. Are performance deficiencies immaterial to the bank's condition?

Electronic Banking

Consider the following procedures at each examination. Examiners are encouraged to exclude items deemed unnecessary. This procedural analysis does not represent every possible action to be taken during an examination. The references are not intended to be all-inclusive and additional guidance may exist. Many of these procedures will address more than one of the Standards and Associated Risks. For the examination process to be successful, examiners must maintain open communication with bank management and discuss relevant concerns as they arise.

PRELIMINARY REVIEW

1 Determine the bank's current and planned electronic banking activities. Consider the following:

1 A Internet banking services (information-only, information-exchange, and transactional services).

1 B Direct dial-up PC banking.

1 C Telephone banking.

1 D Other services (Internet service provider, Web site hosting, trust services, account aggregation, electronic bill presentment).

2 Determine the bank's involvement in development and maintenance of the electronic banking activities. Consider the following:

2 A The location where the Web site is hosted.

2 B The party responsible for maintaining the bank's Web site.

2 C The party responsible for developing the bank's electronic banking system.

2 D The location of the bank's electronic banking system.

2 E The party responsible for maintaining the bank's electronic banking system.

2 F The party responsible for providing customer service (e.g. call center) for electronic banking services.

2 G Whether a third-party provides electronic bill payment processing or any other ancillary services.

3 Determine if the bank operates the Web site, electronic banking system or core data processing system in-house. If so, review the topology (schematic diagram) of the systems and networks, and determine whether there is a direct, on-line connection between the bank's core processing systems and the Internet Web site. Consult an information technology specialist or electronic banking subject matter expert where necessary.

4 If the bank operates the electronic banking system or core data processing system in-house, review the transaction processing flows between the electronic banking system and the bank's core processing systems and identify key control points. Determine whether information is exchanged in a real-time, batch (overnight), or hybrid processing mode.

5 Determine if material changes been made to products, services, or operations since the last examination and if any significant changes are planned in the near future.

6 Determine the significance of the bank's electronic banking activities. Consider the following areas:

6 A Approximate percentages and numbers of customers (e.g. loan and deposit) that regularly use electronic banking products and services.

6 B Lending and deposit volumes generated via Internet applications.

6 C The current monthly transaction and dollar volume for electronic banking services.

7 Review prior examination reports and file correspondence for an overview of any previously identified electronic banking concerns.

8 Review board or committee minutes for evidence of oversight, responsibility, routine management reports, and any identified electronic banking concerns.

9 Review any available audits or reviews of vendors or service providers used by the bank, such as SAS 70 (AICPA Statement of Auditing Standards No. 70, "Reports on the Processing of Transactions by Service Organizations") Reports. Also, review any FFIEC Shared Application Software Review Reports, or FFIEC or agency service provider examination reports from information technology supervision staff.

10 Review the bank's public Web site (or URL, e.g. www.bankname.com).

POLICIES AND PROCEDURES

11 Review the procedures for maintaining the bank's Web site. Consider the following:

11 A Only authorized staff should have the ability to update or change information on the Web site.

11 B Updates of critical information should be subject to dual verification (e.g. interest rates).

11 C Web site information and links to other Web sites should be verified for accuracy and functionality.

11 D Management should implement procedures to verify the accuracy and content of any financial planning software, calculators, and other interactive programs available to customers on an Internet Web site or other electronic banking service.

11 E Links to external Web sites should include a disclaimer that the customer is leaving the bank's site and provide appropriate disclosures, such as noting the extent, if any, of the bank's liability for transactions or information provided at other sites.

12 Review operating policies and procedures to determine, at a minimum, if they include:

12 A Procedures for, and controls, over opening new customer accounts submitted via electronic channels.

12 B Administrative procedures for establishing new accounts in the electronic banking system.

12 C Controls over access to the electronic banking system (e.g., customer passwords, PINs, account numbers).

12 D Appropriate authorizations for electronic debits initiated against other accounts.

12 E Dollar limits on transactions over a given time period (such as per day limit) initiated through the electronic banking service.

12 F Electronic bill payment processing and reconcilement including processing of transactions with insufficient funds.

13 Determine if information security policies and procedures address access to, and protection of, confidential customer information maintained in or obtained via electronic banking products and services.

14 Determine if the bank's policies require formal suspicious activity reporting in the event of computer intrusions affecting the electronic banking system.

15 Determine if business recovery procedures are adequate to address events that could affect the availability of the electronic banking system, such as system outage, natural disaster, or other disruption. Determine if planned recovery times are consistent with the degree of importance of the electronic banking activities to the institution.

16 Determine whether management has established a preparedness plan or an incident response team to handle potential Web site disruptions, malicious tampering with the Web site, or other problem situations.

17 Determine if record retention guidelines are adequate and are updated for source documents supporting electronic banking activities, such as account applications, instructions for account transactions, electronic mail communications, and other records.

INTERNAL CONTROLS AND SECURITY

18 Determine if the bank or the service provider has implemented a firewall to protect the bank's Web site. Determine who installed and configured the firewall, and whether continuing monitoring and maintenance arrangements are in place.

19 If the bank uses a turnkey electronic banking software package or a service provider, review training and security materials provided by the software vendor or service provider. Determine if bank employees are following appropriate security and administrative procedures for their particular system. Consider whether:

19 A Staff are familiar with key controls detailed by the vendor.

19 B Workstations that interface with the service provider's system for administrative procedures or transfer of files and data are kept in a secure location with appropriate password or other access control, dual verification procedures, etc.

20 Assess the adequacy of the process for password administration for access to the electronic banking system (or workstations that interface with a remote service provider system) by bank staff and customers, including:

20 A Procedures to ensure that only authorized staff have access to electronic banking systems and data.

20 B The required length of passwords and avoidance of easily guessed or default passwords, such as social security number or account number.

20 C The procedure for resetting passwords when customers forget their passwords. Determine if the procedure adequately protects against unauthorized access to account numbers and passwords.

20 D Automatic logoff controls for user inactivity.

20 E The number of failed access attempts granted a user before access is denied.

20 F Secure (encrypted) storage of password files and information by the bank or vendor.

21 Determine whether the bank has implemented adequate measures to protect the electronic banking system and associated external communications from computer viruses.

22 If the bank operates electronic banking services in-house, determine whether the bank regularly upgrades electronic banking software to incorporate any upgrades ("patches") provided by the software vendor to address security vulnerabilities.

23 If e-mail is used to communicate with customers, determine whether communications are encrypted or whether customers and employees are advised not to send confidential information via e-mail.

AUDIT AND INDEPENDENT REVIEW

24 Determine if the bank's internal and external audit programs address electronic banking activities and systems, commensurate with the potential financial, operational, and reputational impact and risks to the institution.

25 Determine if the audit program includes reviews of controls over and reconcilement of transactions initiated through the bank's electronic banking system and exception resolution procedures.

26 Determine the level of audit review of service providers' performance relative to contract terms and review audit results.

INFORMATION AND COMMUNICATION SYSTEMS

27 Determine if management accurately reports the Web site address on the Report of Condition.

28 Determine if suspicious activity reports involving electronic banking services are appropriately filed.

29 Determine if adequate procedures are in place for monitoring and addressing customer problems regarding electronic banking products and services, such as difficulties logging in to the system, availability of the system, timeliness of transaction execution, and integrity of customer account information.

30 Determine that adequate summary-level reports showing web-site usage, transaction volume, system problem logs, and transaction exception reports are made available to management with sufficient frequency to keep them informed of system usage trends and customer and operational problems and their resolution or disposition.

31 Determine whether intrusion detection and penetration tests of electronic banking systems have been conducted, and if management has appropriately reviewed the results of such tests.

VENDORS AND OUTSOURCING

32 Determine if management has ensured that the service provider responsible for hosting or maintaining the bank's Web site has implemented:

32 A Controls to protect the bank's Web site from unauthorized alteration and malicious attacks.

32 B Procedures to notify the bank in the event of such incidents.

32 C Regular back-up of Web site information.

33 Determine whether there is a written, signed contract for each significant vendor, service provider, consultant, or contractor relationship involved in development and maintenance of the electronic banking services. Depending on the nature and criticality of the services, consider whether:

33 A Contracts specify minimum service levels and remedies or penalties for non-performance.

33 B Contracts specify liability for failed, delayed, or erroneous transactions processed by the service provider and other transactions where losses may be incurred (e.g. insufficient funds).

33 C Contracts specify contingency plans, recovery times in the event of a disruption, and responsibility for back-up of programs and data.

33 D Contracts specify data ownership, data usage, and compliance with the bank's information security policies.

33 E Contracts provide for access by the bank to the service provider's financial information, audit reports, and security reviews.

33 F Contracts specify insurance to be maintained by the service provider.

33 G Legal counsel has reviewed the contracts to ensure they are legally enforceable and that they reasonably protect the bank from risk.

34 Determine whether bank management and staff conduct initial and periodic due diligence reviews of service providers and assess the adequacy of such reviews. Determine if management has received assurance that the service provider has conducted similar due diligence for any of its supporting agents (i.e., subcontractors, support vendors, and other parties).

35 Assess the adequacy of the bank's vendor oversight program. Determine that responsibilities for vendor management include:

35 A Monitoring whether performance meets service level agreements and communicating any deficiencies to the service provider and to bank management.

35 B Periodically reviewing the financial condition of the service provider and determining whether back-up arrangements are warranted as a result.

35 C Reviewing the service provider's standards, policies and procedures relating to internal controls, security, systems development and maintenance, and business contingency to ensure they meet the bank's minimum guidelines.

35 D Reviewing monitoring reports provided by the service provider relating to transaction volume, response times, availability/downtime, exception reports, and capacity reports and communicating any concerns to bank management and the vendor.

35 E Reviewing third-party audits, SAS 70 reports, and regulatory examination reports pertaining to the service provider, if available, and following up on any findings with the service provider.

35 F Participating in user groups.

35 G Ensuring the bank staff receive adequate training and documentation from the vendor or service provider.

35 H Costs and fees for the service, additional charges for customized services, continuing cost of maintenance and support.

35 I Provisions for subcontracting, including roles and responsibilities for subcontractor performance.

36 If the bank operates a turnkey electronic banking software package, determine whether software is held under a software escrow agreement and that the bank has established procedures to ensure that relevant program files and documentation are kept current and complete.

37 If a vendor maintains the bank's electronic banking system operated by the bank in-house, determine whether the bank ensures adequate controls over the vendor's access (including remote access) to the bank's systems to maintain or upgrade software. Also, determine if:

37 A The bank monitors remote vendor access to its systems through activity logs or other measures.

37 B The vendor's software distribution procedures are adequate and each release is accompanied by sufficient documentation.

38 Determine whether the bank has notified its federal supervisor of applicable service relationships relating to electronic banking as required by the Bank Service Company Act.

BOARD OVERSIGHT

39 Determine whether the board, or an appropriate committee, approves any new or significant enhancements to electronic banking products and services based on a written business plan and risk analysis commensurate with the proposed planned activity. Consider the following:

39 A Whether the service will be designed to provide information or existing services to existing customers, or to attract new customers.

39 B Whether financial incentives will be offered to attract customers through the electronic banking service.

39 C The potential impact of electronic banking products and services on the composition of the bank's customer base.

39 D A review of the projected financial impact of the new service.

39 E Internal controls appropriate for the new product or service.

39 F Whether adequate management reports are provided and subject to periodic review.

39 G The role of audit, compliance, and legal staff.

39 H Whether any new activities are permissible under applicable state and federal banking laws.

39 I The extent of outsourcing and responsibilities for managing vendor and service provider relationships.

40 Determine whether the board provides adequate resources for electronic banking activities. Consider the following items:

40 A Sufficient staff to operate the electronic banking system.

40 B Technical expertise consistent with the complexity of the bank's electronic banking system.

40 C Adequate training and staff development.

41 Determine if management has responded appropriately to the audit recommendations.

42 Determine whether management has evaluated the adequacy of each critical service provider's insurance coverage. Consider the following:

42 A Blanket bond.

42 B Excess liability.

42 C Errors and omissions.

42 D Electronic funds transfer.

42 E Other types of insurance coverage to cover the risks associated with the bank's electronic banking services.

Electronic Banking

Generally, procedures used in the Expanded Analysis should target concerns identified in the Core Analysis and Decision Factors. Expanded procedures associated with Core Analysis and Decision Factors of no concern need not be used. The flexible guidelines specified for the Core Analysis also apply here.

POLICIES, PROCEDURES AND RISK LIMITS

1 Determine why policies do not adequately address electronic banking activities. Evaluate management's plans for incorporating electronic banking activities into operating policies and procedures.

INTERNAL CONTROLS AND SECURITY

2 Determine why the electronic banking internal control environment is inadequate. Consider the following:

2 A Testing of the electronic banking system prior to implementation, including: testing to ensure system reliability and capacity; pilot program to evaluate market impact or feasibility; and security evaluation.

2 B Access rights and authorities of staff. Determine whether access is necessary in all cases and that any changes to access authority are logged and reviewed.

2 C Security, including adequate firewall and intrusion detection systems

2 D The adequacy of business recovery procedures for the electronic banking activities in the event of a system disruption.

3 Review reports summarizing operational and customer problems reported with the electronic banking service. Consider whether the nature and volume of problems regarding electronic banking services indicated recurring problems or management deficiencies.

4 Assess management's plan to correct any identified risks associated with an improper internal control environment.

5 Confirm that safeguards are in place to detect and prevent duplicate transaction within each system and to resolve any exception transactions.

6 Review selected transactions initiated through the electronic banking system, from customer application for on-line services, customer transaction input, posting to customer accounts, to settlement and final disposition. Determine whether policies and risk limits are implemented and enforced as appropriate.

AUDIT AND INDEPENDENT REVIEW

7 Determine why electronic banking activities have not been included in the audit scope.

8 Review any audit findings not corrected by management and assess their significance for the electronic banking operations.

INFORMATION AND COMMUNICATION SYSTEMS

9 Determine why management reports do not provide assurance that the bank is in compliance with approved policies and regulatory requirements.

VENDORS AND OUTSOURCING

10 Assess the quality of service and reliability of risk controls provided by the vendor. Determine whether lack of appropriate contract terms or due diligence exposes the bank to undue risk, based on the importance of the services provided and the potential liability involved.

11 Determine the effectiveness of the bank's ability to resolve problems with the vendor, or whether other measures, such as escalation of communications, penalties, or contract termination should be considered.

12 Review reports used to monitor the vendor's service level performance. Determine whether any concerns have arisen in vendor operations that have significantly affected the bank's ability to manage its operational risks. Consult an information technology specialist to determine whether contact with the vendor may be appropriate to obtain further information on the vendor's operations.

BOARD OVERSIGHT

13 Determine the impact of the lack of effective oversight and risk management program for electronic banking activities on the bank, based on the significance of the services offered to the bank's risk profile. Evaluate management's plans for correcting weaknesses, and determine if the plans are reasonable.

Electronic Banking

Impact Analysis reviews the impact that deficiencies identified in the Core and Expanded Analysis and Decision Factors have on the bank's overall condition. Impact Analysis also directs the examiner to consider possible supervisory options.

1 Determine the impact electronic banking activities have on the bank's financial condition.

2 Consult with an electronic banking subject matter expert or information technology specialist for assistance when determining the impact of material weaknesses noted in electronic banking activities.

3 Discuss electronic banking deficiencies with management and seek commitment to remedy the electronic banking exposure and control deficiencies.

4 Determine the need for administrative and enforcement actions, formulate specific recommendations and advise the appropriate supervisors of the nature of the concerns.

5 Discuss the possibility of administrative and enforcement actions with executive management and the board of directors.

6 Investigate potential recommendations for civil money penalties and remedial action.